Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	CyberSource Corporation		DBA (doing business as):	CyberSource, Authorize.Net, CyberSource KK, and CyberSource Managed Hosting	
Contact Name:	La Tanya Timmons		Title:	Regulatory and Risk Governance, Sr. Director	
Telephone:	+1 (650) 432-2331		E-mail:	latimmon@visa.com	
Business Address:	800 Metro Center Blvd.		City:	Foster City	
State/Province:	CA	Country:	USA	Zip:	94404
URL:	https://www.visa.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Trustwave Holdings, Inc.				
Lead QSA Contact Name:	Pablo Gomezsolis		Title:	Sr. Security Consultant	
Telephone:	+1 (312) 873-7500		E-mail:	pgomezsolis@trustwave.com	
Business Address:	70 West Madison Street, Suite 600		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60602
URL:	https://www.trustwave.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Payment Gateway, Managed Hosting

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☒ POS / card present
☒ Hardware	☐ IT support	☒ Internet / e-commerce
☒ Infrastructure / Network	☐ Physical security	☒ MOTO / Call Center
☒ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☒ Storage	☐ Other services (specify):	☐ Other processing (specify):
☒ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		
☐ Account Management	☒ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☒ Billing Management	☐ Loyalty Programs	☐ Records Management
☒ Clearing and Settlement	☒ Merchant Services	☒ Tax/Government Payments
☒ Network Provider		
☒ Others (specify): Tokenization Services		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	Not Applicable	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	CyberSource, along with Authorize.Net, CyberSource KK, and CyberSource Managed Hosting, are wholly owned subsidiary of Visa, Inc. and is fully integrated into the Visa environment. **CyberSource** CyberSource stores cardholder data as a service provider engaged in operating an electronic payments network. CyberSource accepts card-present, card-not-present, and PIN/debit transaction data in the course of conducting their business. CyberSource's services include Billing Management, Clearing and Settlement, Fraud and Chargeback, Merchant Services, Network provider, as such, CyberSource stores cardholder data (Cardholder Name, PAN and expiration date, In Databases utilizing AES 256-bit encryption), and Tokenized PAN, as part of its business processes. All data storage is in secure networks located within the OCC, OCE data centers. CyberSource receives cardholder data (PAN, Expiration Date, Cardholder Name and Card Security Codes [CVV2, CVC2, CID, CAV2]) via TLS 1.2 (AES 256-bit) connections and CyberSource transmits cardholder data (Full track data, PIN Block, and Card Security Code [CVV2, CVC2, CID, CAV2]) via TLS v1.2 (AES 256-bit) or private MPLS circuits (depending on processor), to payment processors as part of the authorization process. SFTP is also used to transmit cardholder data (PAN) to the processors as part of the settlement process. CyberSource receives cardholder data (PAN, Expiration Date, Cardholder Name and Card Security Codes [CVV2, CVC2, CID, CAV2]) via phone calls made from the customer to the call centers and entered in the applications (protected via HTTPS TLS 1.2 AES 256-bit) by the call agents. **Authorize.Net** Authorize.Net stores transactional details as part of the authorization process. Cardholder data (PAN, Expiration Date, Cardholder Name), and card security codes (CVV2, CVC2, CID, CAV2) is passed to the respective processor, only held in volatile memory, and purged upon transmission to the processor (overwritten with the next transaction). Card security codes (CVV2, CVC2, CID, CAV2) are never stored on Authorize.Net systems. The transactional details (PAN, Expiration Date,

	Cardholder Name), saved are immediately encrypted by a FutureX encryption appliance, using AES 256-bit encryption. The encrypted credit card transactional data (PAN, Expiration Date, Cardholder Name), is then stored on a relational database. Authorize.Net receives cardholder data (PAN, Expiration Date, Name, Card security Codes [(CVV2, CVC2, CID, CAV2]) via TLS 1.2 (AES 256-bit) connections and transmits cardholder data via TLS v1.2 (AES 256-bit) or private MPLS circuits (depending on processor), to payment processors as part of the authorization process. **CSKK** CyberSource KK (CSKK) itself does not store card or other data used in transactions, instead relying on the CyberSource Corporation systems for this function. However, there is some card data, including PAN, cardholder name, and expiry date, that is stored as hard copy (paper) in the CSKK office. **CyberSource Managed Hosting** CyberSource Managed Hosting provides physical hosting and application development for their customers but is not a shared hosting provider. CyberSource Managed Hosting stores credit card data (PAN, In Databases utilizing 3DES 192-bit encryption) within their hosted network environment. Any customer data traffic is stored and processed by CyberSource. CyberSource Managed Hosting sends credit card data (Full track, Track equivalent data, PAN, expiry, Cardholder Name, card security codes [CVV2, CVC2, CID, CAV2], PIN block) to CyberSource only. CyberSource Managed Hosting receives cardholder data via TLS 1.2 (AES 256-bit) connections and transmits cardholder data (Full track, Track equivalent data, PAN, expiry, Cardholder Name, card security codes [CVV2, CVC2, CID, CAV2], PIN block) via TLS 1.2 (AES 256-bit) to CyberSource. CyberSource Managed Hosting is a business unit within CyberSource.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Corporate Office	3	Foster City, CA, USA Bellevue, WA, USA Yokohama, Japan
Data Center	2	Highlands Ranch, CO, USA Ashburn, VA, USA
Call Center	5	Austin, TX USA Lehi, UT USA Manila, Philippines Reading, UK Singapore, Singapore

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
ANET Mobile Payment Application	N/A	Bespoke	☐ Yes ☒ No	N/A

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The following networks were defined in the cardholder data environment: • Corporate • Tier0 The following zones, segmented by firewalls, were defined: • Perimeter Zone (first tier DMZ) • Business Zone (second tier with application hosting) • Restricted Zone (third tier with cardholder data storage) The following critical systems reside in the cardholder data environment: • Stateful Inspection Firewall, router and switches: for network protection and CDE definition, traffic directing and data forwarding.

- Load Balancers.
- Applications (Web Interfaces) to support the CyberSource business processes.
- Servers to support the receipt of cardholder data and the transmission of cardholder data to processor.
- Databases that store cardholder data and information to support business processing.
- File integrity monitoring to validate the integrity of the operating system, database and application files.
- Log aggregation using centralized aggregation, long-term retention of system and application logs for analysis.
- Hardware Security Solutions (HSM) for key management and key management functionality.
- Change Management application to manage, document and track changes to the environment and manage required approvals.
- Data Loss Prevention (DLP) for data protection including scanning and analysis of the network traffic.
- Anti-Virus software to detect and remove computer viruses and other virus-related software.
- Application code scanning to ensure application code meets industry best practices and support peer review as well as enterprise coding standards.
- Wireless controllers which support the CyberSource wireless environment and provide controls to ensure wireless traffic is secure.

Processor connections:

- Directly connected for processing and transmission: AIBMS, Alipay International, Alipay Domestic, Amex Brighton, Amex Direct, Atos, Barclays, BML Direct, Braspag, Brazil Boleto, Cardnet/Omnipay FDI, Cielo, Citimb, CitiIndia, CMCIC, Commercio Latino, Ctp, CtV, FDC Compass, FDC Germany, FDC Nashville, FDC South, FDC South Reformatter, FDI Australia, FDI Global, First Vision, GlobalCollect, FPN, HBoS, HSBC,

		JCN Gateway, Kcp, Latina MCC, Litle, Lynk, Migs, Mollie, Moneris, Omni Ireland, OmniPay Direct, Payease China, Payease Direct, RBS WorldPay, SmartPay, Sofort, uatp, VAA, Vantiv, Vital. Directly connected for transmission: Fair Isaac Corporation.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*		☒ Yes ☐ No

Part 2f. Third-Party Service Providers		
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?		☐ Yes ☒ No
If Yes:		
Name of QIR Company:	Not Applicable	
QIR Individual Name:	Not Applicable	
Description of services provided by QIR:	Not Applicable	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?		☒ Yes ☐ No
If Yes:		
Name of service provider:	**Description of services provided:**	
Fair Isaac Adeptra Inc. (Fair Issac Corporation)	Provides Credit checks on potential customers for merchants	
Note: *Requirement 12.8 applies to all entities in this list.*		

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website*.

Name of Service Assessed:	Payment Gateway, Managed Hosting

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	
Requirement 2:	☐	☒	☐	Req. 2.2.3 – Not applicable. CyberSource does not have any services, protocols, or daemons that are considered to be insecure. Req. 2.6 – Not applicable. CyberSource is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Req. 3.4.1 – Not applicable. CyberSource does not utilize disk encryption technologies to meet the storage encryption requirement. Req. 3.6.6 – Not applicable. CyberSource does not use manual clear-text cryptographic key-management operations.
Requirement 4:	☒	☐	☐	
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Req. 6.4.6 – Not applicable. No system components were significantly changed since the previous assessment.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Req. 8.1.5 – Not applicable. CyberSource does not use any vendor accounts. Req. 8.5.1 – Not applicable. CyberSource does not control account information for its customer environment.

Requirement 9:	☐	☒	☐	Req. 9.6.2 – Not applicable. CyberSource does not send media outside their facilities. Req. 9.6.3 – Not applicable. CyberSource does not deliver CHD that is in removable media anywhere outside their facilities. Req. 9.9 – Not applicable. CyberSource does not maintain any payment card devices. Req. 9.9.1 – Not applicable. CyberSource does not maintain any payment card devices. Req. 9.9.2 – Not applicable. CyberSource does not maintain any payment card devices. Req. 9.9.3 – Not applicable. CyberSource does not maintain any payment card devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Req. 11.2.3 – Not applicable. No system components were significantly changed that would require immediate internal or external scans since the previous assessment.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Not applicable. CyberSource is not a shared hosting provider.
Appendix A2:	☐	☐	☒	Not applicable. CyberSource does not have POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	August 6, 2020	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *August 6, 2020.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *CyberSource Corporation* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys, Inc.*

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

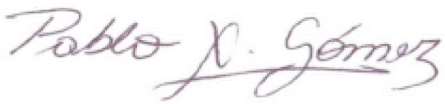
[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 8-13-20
Service Provider Executive Officer Name: Sunil Seshadri	*Title:* SVP, CISO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	The Trustwave Holdings, Inc. QSA (Pablo Gomezsolis) performed all scoping, interviews with Visa personnel, observation of in-place controls, evaluation of controls and report documentation for this assessment.



Signature of Duly Authorized Officer of QSA Company ↑	*Date:* August 6, 2020
Duly Authorized Officer Name: Pablo Gomezsolis	*QSA Company:* Trustwave Holdings, Inc.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Jason Miles-Wynter-Pink – Lead ISA. Reviewed, gathered, and provided support evidence.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐